

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

STEVE WAITHE,

Defendant

) Criminal No. 21cr10342
)

) Violations:
)

) Counts One through Twelve: Wire Fraud
) (18 U.S.C. § 1343)
)

) Count Thirteen: Cyberstalking
) (18 U.S.C. § 2261A(2)(B))
)

) Count Fourteen: Conspiracy to Commit
) Computer Fraud
) (18 U.S.C. § 371)
)

) Count Fifteen: Computer Fraud, Aiding and
) Abetting
) (18 U.S.C. §§ 1030(a)(4) and 2)
)

) Wire Fraud Forfeiture Allegation:
) (18 U.S.C. § 981(a)(1)(C) and
) 28 U.S.C. § 2461(c))
)

) Computer Fraud Forfeiture Allegation:
) (18 U.S.C. §§ 982(a)(2)(B) & 1030(i))
)

INDICTMENT

At all times relevant to this Indictment:

General Allegations

1. Steve WAITHE (“WAITHE”) resided in or around the District of Massachusetts and the Northern District of Illinois. From on or about October 11, 2018 until in or about February 2019, WAITHE was employed as a coach of the men’s and women’s track and field team at Northeastern University (“Northeastern”).

2. Instagram is a social media application and service offered by Meta Platforms Inc. (formerly Facebook Inc.) that enables users to, among other things, share photos and videos and

to communicate with one another through “direct messages” in the application. Direct messages can be comprised of text, images, and/or videos. Instagram servers are used in and affecting interstate commerce and are located outside of the District of Massachusetts.

3. Snapchat is a social media application and service offered by Snap Inc. that allows users to share photos, videos, and messages – commonly called “snaps” – with other users. Snaps can be directed privately to selected contacts or to a more public “story.” Unless the sender or recipient chooses to save a snap, the snap is automatically deleted, either after the content is sent or after it is opened. Snapchat also offers users the ability to save photos and videos in a private, passcode-protected portion of the application called “My Eyes Only.” Snapchat utilizes servers that are used in and affecting interstate and foreign commerce and are located outside of the District of Massachusetts.

4. Victims 1-6 were members of the Northeastern track and field team who resided in or around the District of Massachusetts in 2020.

Scheme to Defraud

5. From at least as far back as February 2020 through in or about April 2021, WAITHE engaged in an evolving pattern of fraudulent conduct to deceive, or attempt to deceive, as many women as he could, in Massachusetts and across the country, into sending him nude and/or semi-nude photos of themselves. WAITHE’s conduct included the use of sham Instagram accounts, as well as the fabrication of two female identities, “Katie Janovich” and “Kathryn Svoboda,” through which WAITHE contacted prospective victims and attempted to dupe them into sending compromising photos.

6. During his tenure as a track coach at Northeastern, WAITHE began engaging in conduct that formed the foundation for his fraudulent scheme. For example, during track and

field practices and/or meets, WAITHE requested the use of the cell phones of female student-athletes under the pretense of “filming their technique.”

7. At various practices and/or meets, WAITHE was observed “scrolling” through the phones of female student-athletes and at times left the track while in possession of their phones.

8. In or about February 2020, approximately one year after the end of WAITHE’s employment at Northeastern, WAITHE began contacting female then-current and/or former members of the Northeastern track and field team through anonymized Instagram accounts.

9. Through the course of his scheme, WAITHE created a series of Instagram accounts with anonymized display names or handles such as “anon.4887” and variations of the phrase “Privacy Protector,” and utilized Instagram’s “direct message” function to contact prospective victims.

10. In direct messages to six female then-current or former members of the Northeastern track and field team (“Victims 1-6”), WAITHE’s communications followed the same basic pattern:

- a. Sending compromising photos of the victim and/or others;
- b. Claiming that the photos had been discovered online;
- c. Offering to “help” the victim remove the photos from the internet, usually through a “reverse image search”; and
- d. Requesting additional nude and/or semi-nude photos of the victim to assist him in doing so.

11. For example, on or about February 13, 2020, WAITHE sent the following direct message utilizing the Instagram account “anon.4887” to Victim 1, a female then-current or former member of the Northeastern track and field team: “Hey [Victim 1], my name is Katie. I

think you went to Northeastern. But I just wanted to let you know that VSCO [h]ad a page called hacked nudes where I saw some that looked like you ... So I just wanted to let you know. Are these you?"

12. WAITHE then sent direct messages to Victim 1 that contained nude and/or semi-nude photographs depicting Victim 1, followed by a direct message that asked, "Were those you? I can look for ones that look like you if that makes sense." WAITHE also messaged, "I'll send all the personal ones if you send me you that's the only way" and "But only if you send yours."

13. In furtherance of the scheme, WAITHE sent direct messages to prospective victims from over a dozen anonymized Instagram accounts. WAITHE sent over 100 direct messages to Victims 1-6 that contained nude and/or semi-nude images depicting Victims 1-6 and others. Victims 1-6 did not send any nude or semi-nude images of themselves to WAITHE.

14. In or about March 2020, WAITHE began contacting prospective victims while pretending to be one of at least two fabricated female personas with the names "Katie Janovich" and "Kathryn Svoboda."

15. In furtherance of the scheme, WAITHE created and utilized Google email ("Gmail") addresses in the names of "Katie Janovich" and "Kathryn Svoboda."

16. In emails to prospective victims, WAITHE – posing as "Katie" or "Kathryn" – described a phony "body development study" involving research on athletes' bodies and requested information relating to height, weight, body fat, and diet habits.

17. While posing as "Katie Janovich" and/or "Kathryn Svoboda," WAITHE requested that victims send photos of themselves in various stages of undress purportedly to "track their progress" during the "body development study."

18. For example, on or about March 4, 2020, WAITHE posed as “Katie Janovich” and utilized the Google email account “janovichkatie@gmail.com” to send an email to Victim 7, which began, “Hey [Victim 7]! My name is Katie, Steve told me to reach out to you in hopes for you[] to help us with our research! We have been compiling data and results for almost 4 years now and we have been trying to get as many athletes from as many sports and disciplines as possible.” WAITHE emphasized the importance of receiving nude and/or semi-nude photographs, stating: “Most important. Pictures of you from your competition days preferably in a uniform or bathing suit to show as much skin as possible. And then the same now. Most women have just sent a bunch of pictures in a bra and a thong because it shows the most. Regular deep cut bras are best if you want to go topless women have done that too because the easiest places the body usual[ly] shows changes is the butt and breasts.”

19. WAITHE attached to the email 29 nude and/or semi-nude photos of an unknown woman and stated, “I’m gonna attach some examples for you. Please do not share them with anyone. Send whatever you’re comfortable with but remember the more skin the better[.]”

20. In furtherance of the scheme to defraud, WAITHE posed as “Katie” and “Kathryn” to communicate with dozens of women. While some women ignored WAITHE’s emails, at least 17 responded, sending over 350 nude and/or semi-nude photographs to the “Katie Janovich” and “Kathryn Svoboda” email accounts.

21. From at least as far back as February 2020 until in or about April 2021, WAITHE defrauded, and attempted to defraud, at least 49 women, including women who reside in California, Colorado, Connecticut, Florida, Illinois, Indiana, Maryland, Massachusetts, Michigan, Minnesota, New Jersey, Pennsylvania, South Carolina, Texas, and Virginia.

Cyberstalking

22. From on or about June 21, 2020 through at least on or about October 3, 2020, WAITHE engaged in a pattern of harassment and intimidation with respect to Victim 6, a then-current or former member of the Northeastern University track and field team.

23. WAITHE's conduct with respect to Victim 6 included sending messages and stolen or otherwise-compromised nude photos depicting Victim 6 via Instagram direct messages; obtaining, or conspiring to obtain, unauthorized access to her Snapchat account; stealing, or conspiring to steal, private photos contained in her Snapchat account; sending the private photos via Instagram direct message to Victim 6's boyfriend; and sending additional text messages to Victim 6 from an anonymized phone number.

24. For example, on or about June 21, 2020, at approximately 12:34 AM, WAITHE began sending direct messages to Victim 6 from the Instagram account "privacyprotector."

25. In his messages to Victim 6, WAITHE sent approximately seven nude photos depicting both Victim 2 and Victim 6 under the pretense that he could help Victim 6 determine the origin of the photos and assist in having them removed from the internet. The photos sent to Victim 6 had been stored on her cellphone in Fall 2018 when WAITHE was her track and field coach at Northeastern.

26. On or about October 3, 2020, Victim 6 received text messages from four unknown numbers purporting to be sent from the "Snapchat Support Team" and experienced a breach of her Snapchat account, as described in further detail below. WAITHE orchestrated and otherwise participated in the breach of Victim 6's Snapchat account.

27. In the evening on or about October 3, 2020, WAITHE began sending direct messages to Victim 6's boyfriend through the Instagram account "pvcyprotect." In his first

message, sent at approximately 9:06 PM, WAITHE wrote, “I wanted to make you aware that someone hacked your girlfriend’s snapchat account and will leak it soon. I need your help to assure this does not happen.”

28. On or about October 3, 2020, WAITHE used the “pvcyprotect” Instagram account to send two nude photos depicting Victim 6 to Victim 6’s boyfriend that had been stored in the private “My Eyes Only” folder in Victim 6’s Snapchat account. WAITHE wrote, “Do these look familiar?” and “Please let me know asap.”

29. On or about October 3, 2020, at approximately 9:20 PM, WAITHE utilized an anonymized phone number to send text messages to Victim 6, including a message containing another photograph depicting Victim 6, as well as the question, “Is this you?”

Overview of Conspiracy to Commit Computer Fraud

30. In or about May 2020, WAITHE began formulating a plot to hack into victims’ Snapchat accounts by posting on a website, “LeakedBB.com,” requesting advice on “How to hack Snapchat.”

31. By May 2020, WAITHE had already created and utilized a series of anonymized or disguised Instagram and Google accounts to conceal his identity and attempt to deceive women into sending him nude and/or semi-nude photos of themselves.

32. In or about October 2020, WAITHE’s efforts to obtain unauthorized access to victims’ Snapchat accounts escalated when he began contacting one or more other individuals to assist in the endeavor.

33. For example, WAITHE contacted someone who had posted online about his ability to hack into Snapchat accounts (“CC-1”), and WAITHE provided him with the Snapchat usernames and corresponding phone numbers for over a dozen women.

34. WAITHE and CC-1 obtained access to the Snapchat accounts of one or more victims and downloaded or otherwise copied certain contents of the accounts, including nude and/or semi-nude photos stored in the accounts.

35. WAITHE downloaded the stolen images, stored them both in cloud-based storage and on an SD memory card, and later offered to “trade” photos of one or more victims to others on the LeakedBB website.

Object and Purpose of Conspiracy

36. The principal object of the conspiracy was to commit computer fraud, in violation of Title 18, United States Code, Section 1030(a)(4), by accessing a protected computer, to wit, the servers utilized by Snap Inc., without authorization to obtain a thing of value. The principal purpose of the conspiracy was for WAITHE to obtain nude and/or semi-nude photos of the victim(s) to keep for himself and to sell and/or trade to others.

Manner and Means of Conspiracy

37. Among the manner and means by which WAITHE, together with others known and unknown to the Grand Jury, carried out the conspiracy to commit computer fraud were the following:

- a. Contacting CC-1 to request assistance hacking into Snapchat accounts;
- b. Providing CC-1 with the Snapchat usernames and corresponding phone numbers for at least 15 prospective victims, including Victim 6;
- c. Downloading the images obtained by CC-1 through unauthorized access of Victim 6’s Snapchat account; and
- d. Making one or more payments to CC-1 in exchange for CC-1’s assistance in obtaining unauthorized access to, as well as the contents of, Victim 6’s

Snapchat account.

Overt Acts in Furtherance of Conspiracy

38. On various dates between in or about May 2020 and in or about October 2020, WAITHE committed and caused to be committed the following overt acts in furtherance of the conspiracy to commit computer fraud:

39. In or about May 2020, WAITHE posted on the website "LeakedBB.com" a request for advice or information regarding "How to hack Snapchat."

40. On or about October 2, 2020, WAITHE conducted internet searches for, among other things, "how to hack snapchat with a username and phone number" and visited webpages entitled, "How to Hack Someones Snapchat the Easy Way" and "How to Hack Someones Snapchat Account Password Online."

41. On or about October 3, 2020, WAITHE contacted CC-1, an individual who had posted on the LeakedBB website about his ability to hack into Snapchat accounts.

42. On or about October 3, 2020, WAITHE provided CC-1 with the Snapchat usernames and phone numbers of approximately 15 women, including the username and phone number of Victim 6.

43. On or about October 3, 2020, CC-1 utilized one or more anonymized phone numbers to send text messages to Victim 6 pretending to be the "Snapchat Support Team" and requesting a six-digit security code, as well as a four-digit passcode.

44. Using information provided by WAITHE and obtained from Victim 6, on or about October 3, 2020, CC-1 accessed Victim 6's Snapchat account, including her private "My Eyes Only" folder.

45. On or about October 3, 2020, CC-1 sent WAITHE a message on the LeakedBB

website with Victim 6's Snapchat username and a link to a cloud storage folder.

46. On or about October 3, 2020 WAITHE responded, "Hell yeah man keep it coming I'll pay you gladly. How do you accept money?"

47. On or about October 3, 2020, WAITHE sent a payment to a Google Pay account associated with CC-1.

48. On or about October 12, 2020, WAITHE posted on the LeakedBB website an offer to "trade" photos of Victim 6.

COUNTS ONE THROUGH TWELVEWire Fraud
(18 U.S.C. § 1343)

The Grand Jury charges:

49. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 21 of this Indictment.

50. From in or about February 2020 through in or about April 2021, in the District of Massachusetts and elsewhere, the defendant,

STEVE WAITHE,

having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, as set forth below:

Count	Approximate Date	Description
1	February 13, 2020	Instagram direct message from anon.4887 account to Victim 1 claiming to have found “hacked nudes” online
2	February 13, 2020	Instagram direct message from anon.4887 account to Victim 1 containing one or more nude and/or semi-nude photos of Victim 1
3	February 13, 2020	Instagram direct message from anon.4887 account to Victim 1 requesting additional nude and/or semi-nude photos of Victim 1
4	June 12, 2020	Instagram direct message from Privacy Protector account to Victim 2 containing one or more nude and/or semi-nude photos of Victim 2
5	June 12, 2020	Instagram direct message from Privacy Protector account to Victim 2 asking if Victim 2 would like assistance removing nude and/or semi-nude photos from the internet
6	June 30, 2020	Instagram direct message from privacyprotect1 account to Victim 3 containing one nude and/or semi-nude photo of Victim 3

7	June 30, 2020	Instagram direct message from privacyprotect1 account to Victim 3 offering assistance in removing nude and/or semi-nude photos from the internet
8	July 26, 2020	Instagram direct message from theprivacyprotector account to Victim 4 containing one nude and/or semi-nude photo of Victim 4
9	July 26, 2020	Instagram direct message from theprivacyprotector account to Victim 4 suggesting that Victim 4 send additional nude and/or semi-nude photos for a “reverse image search”
10	July 26, 2020	Instagram direct message from theprivacyprotector account to Victim 5 purporting to notify Victim 5 that nude and/or semi-nude photos of her had been found on the internet
11	July 26, 2020	Instagram direct message from theprivacyprotector account to Victim 5 containing one nude and/or semi-nude photo of Victim 5
12	July 27, 2020	Instagram direct message from theprivacyprotector account to Victim 5 stating that five of Victim 5’s teammates were depicted in nude and/or semi-nude photos found on the internet

All in violation of Title 18, United State Code, Section 1343.

COUNT THIRTEEN
Cyberstalking
(18 U.S.C. § 2261A(2)(B))

The Grand Jury further charges:

51. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 4, 22 through 29, 32 through 35, and 37 through 48 of this Indictment.

52. From in or about June 2020 through in or about October 2020, in the District of Massachusetts and elsewhere, the defendant,

STEVE WAITHE,

did, with intent to harass and intimidate another person, use interactive computer services, electronic communications services, and electronic communication systems of interstate commerce, specifically text messages, social media direct messages, emails, and online postings, to engage in a course of conduct that caused, attempted to cause, and would be reasonably expected to cause substantial emotional distress to Victim 6.

All in violation of Title 18, United States Code, Section 2261A(2)(B).

COUNT FOURTEEN

Conspiracy to Commit Computer Fraud
(18 U.S.C. § 371)

The Grand Jury further charges:

53. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 4 and 30 through 48 of this Indictment.

54. On or about October 3, 2020, in the District of Massachusetts and elsewhere, the defendant,

STEVE WAITHE,

conspired with CC-1 and others known and unknown to the Grand Jury, to commit offenses against the United States, to wit, computer intrusion, in violation of Title 18, United States Code, Section 1030(a)(4), that is, to knowingly access a protected computer without authorization, with intent to defraud, and by means of such conduct to further the intended fraud and obtain a thing of value;

All in violation of Title 18, United States Code, Section 371.

COUNT FIFTEEN

Computer Fraud; Aiding and Abetting
(18 U.S.C. §§ 1030(a)(4) and 2)

The Grand Jury further charges:

55. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 4 and 30 through 48 of this Indictment.

56. On or about October 3, 2020, in the District of Massachusetts and elsewhere, the defendant,

STEVE WAITHE,

together with CC-1 and others known and unknown to the Grand Jury, did knowingly access a protected computer without authorization, with intent to defraud, and by means of such conduct did further the intended fraud and obtain a thing of value, to wit, nude and semi-nude images of Victim 6.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

WIRE FRAUD FORFEITURE ALLEGATION
(18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

1. Upon conviction of one or more of the offenses in violation of Title 18, United States Code, Section 1343, set forth in Counts One through Twelve, the defendant,

STEVE WAITHE,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses.

2. If any of the property described in Paragraph 1, above, as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), as a result of any act or omission of the defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 1 above.

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c).

COMPUTER FRAUD FORFEITURE ALLEGATION
(18 U.S.C. §§ 982(a)(2)(B) & 1030(i))

The Grand Jury further finds:

1. Upon conviction of one or more of the offenses in violation of Title 18, United States Code, Sections 371, 1030(a), and 2, set forth in Counts Fourteen and Fifteen, the defendant,

STEVE WAITHE,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B) and 1030(i), any property constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses; and, pursuant to Title 18, United States Code Section 1030(i), any personal property used, or intended to be used, to commit, or to facilitate the commission of, such offenses and any property, real or personal, constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses. The property to be forfeited includes, but is not limited to, the following assets:

- a. One black Google Pixel 5 cell phone;
- b. One HTC cell phone, model no. 0P6B130;
- c. One Samsung Notebook laptop, model number XE500C12, bearing serial number 1BEF9FAG419150B;
- d. One Apple iPad bearing serial number F6QRG13RFK11;
- e. One Seagate Free Agent Desktop HD bearing serial number 6QF0PMVD; and
- f. One SanDisk 64 GB SD memory card bearing serial number 058F64656471.

2. If any of the property described in Paragraph 1, above, as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), as a result of any act or omission of the defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 18, United States Code, Sections 982(b)(2) and 1030(i)(2), each incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 1 above.

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

A TRUE BILL


FOREPERSON


ADAM W. DEITCH
ASSISTANT UNITED STATES ATTORNEY
DISTRICT OF MASSACHUSETTS

District of Massachusetts: NOVEMBER 30, 2021
Returned into the District Court by the Grand Jurors and filed.

/s/ Lisa Belpedio at 4:00 pm
DEPUTY CLERK